

	POLİTİKA	SAYFA NO	1/2
		DOKÜMAN NO	BGYS.PLT.25
		YAYIN TAR.	07.01.2019
		REVİZYON NO	01
		REVİZYON TARİHİ	06.03.2023
KONU	ZARARLI YAZILIMLARA KARŞI KORUNMA POLİTİKASI		

Revizyon İzleme Tablosu		
Rev. No	Rev. Tarihi	Açıklama
01	06.03.2023	Cumhurbaşkanlığı Bilgi Güvenliği Rehberi Uyum çalışmaları kapsamında değişikliğe gidilmiştir.

1. AMAÇ

Bu politika **Afyon Kocatepe Üniversitesi** yazılımlarının ve bilgilerinin bütünlüğünü korumak amacıyla hazırlanmıştır.

2. KAPSAM

Bu politika **Afyon Kocatepe Üniversitesinde** kurumsal iletişim ağına bağlanan tüm kullanıcıların sahip olduğu kurumsal veya kişisel cihaz/cihazları için geçerlidir.

3. UYGULAMA

- Bir virüsün varlığından şüphelenen bir kullanıcı;
 - İlgili bilgisayarı kapatmalı,
 - Bilgisayarın ağ bağlantısını kopartmalı,
 - Bu bilgiyi Bilgi İşlem Daire Başkanlığı ilgili uzman personeline iletmelidir.
- Kurumsal ağa bağlanan tüm cihazlara antivirüs programı yüklenmelidir ve devre dışı bırakılmamış olmalıdır.

Revizyon Nedeni:	Hazırlayan	Kontrol Eden	Onaylayan
Cumhurbaşkanlığı Bilgi Güvenliği Rehberi Uyum çalışmaları kapsamında değişikliğe gidilmiştir.	BGYS Yöneticisi	BGYS Üst Yönetim Temsilcisi (Bilgi İşlem Daire Başkanı)	Üst Yönetim Rektör

	POLİTİKA	SAYFA NO	2/2
		DOKÜMAN NO	BGYS.PLT.25
		YAYIN TAR.	07.01.2019
		REVİZYON NO	01
		REVİZYON TARİHİ	06.03.2023
KONU	ZARARLI YAZILIMLARA KARŞI KORUNMA POLİTİKASI		

- Dış kaynaklı dokümanlar, diğer dokümanların bulunduğu ortama aktarılmadan önce en güncel virüs tanımlamalarını içeren bir antivirüs programı ile taranmalıdır. Eğer doküman şifrelendirilmişse, doğrulanmadan önce şifresi kaldırılmalıdır.
- Yedek alınan dokümanların kopyası bir iş istasyonuna veya sunucuya kopyalanmadan önce bir antivirüs programı ile taranmalıdır.
- Kullanıcılar, mevcut bilgi sistemlerinin normal işleyişine zarar verebilecek, kopyalanmasına neden olacak kodlar yazmamalı, yaymamalı veya yönetmemelidir.
- Kuruma ait olmayan sitelerden indirilen yazılımlardan kullanıcı sorumludur. Yükleme işleminin tüm aşamalarından, yazılımın bütünlüğü, virüs taraması, lisans durumu vb. kontrollerinin yapılmasından kullanıcı yükümlüdür.
- Zararlı yazılımdan korunma uygulamalarına ait politikalar merkezi olarak yönetilmelidir.
- AKÜ Bilişim kaynakları kullanım politikasına göre Bilgi İşlem Daire Başkanlığı, bilgisayar ağında oluşabilecek güvenlik açıklarını asgari düzeye indirebilmek için, içerik sağlayıcılarına ve kullanıcılarına güvenlik yazılımları (antivirus, antispam ve kişisel güvenlik yazılımı) temin eder ve kullanıcıları bilgilendirir.

4. YAPTIRIM

Bu politikaya uygun olarak davranmayan kullanıcılar hakkında mevzuatlarda belirtilen hükümler ve kurumun disiplin prosedürü uygulanır.

Revizyon Nedeni:	Hazırlayan	Kontrol Eden	Onaylayan
Cumhurbaşkanlığı Bilgi Güvenliği Rehberi Uyum çalışmaları kapsamında değişikliğe gidilmiştir.	BGYS Yöneticisi	BGYS Üst Yönetim Temsilcisi (Bilgi İşlem Daire Başkanı)	Üst Yönetim Rektör